

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

Remarks

The present amendment responds to the Official Action mailed December 4, 2003. The Official Action rejected claims 1 and 3 under 35 U.S.C. §103(a) based on Haitzuka et al. U.S. Patent No. 6,366,298 ("Haitzuka") in view of Robinson U.S. Patent No. 5,918,014 ("Robinson") and further in view of Shear et al. U.S. Pat. App. Pub. No. US 2003/0041239 A1 ("Shear"). Claims 4, 6, and 7 were rejected under 35 U.S.C. §103(a) based on Haitzuka in view of Robinson and Shear and further in view of Kunzinger et al. U.S. Patent No. 6,405,222 ("Kunzinger"). Claims 8, 9, and 11-13 were rejected under 35 U.S.C. §103(a) based on Haitzuka, Robinson, Shear, Kunzinger and further in view of Davis et al. U.S. Patent No. 5,796,952 ("Davis"). Claims 14 and 19 were rejected under 35 U.S.C. §103(a) based on Haitzuka, Robinson, Shear, Kunzinger, Davis, and further in view of Thomas U.S. Patent No. 6,128,663 ("Thomas"). Claims 10, 15-18, and 20-22 were rejected on the "same rationale" as claims 1, 3, 4, 6-9 and 11-14. These issues are addressed below following a brief discussion of the present invention to provide context.

No claims have been amended by this response. Claims 1, 3, 4, and 6-22 are presently pending.

The Present Invention

The present invention addresses the needs of web content providers (1) to measure the effectiveness of their website in order to compete and (2) to focus their content to their subscribers or future subscribers while (3) maintaining the privacy of individuals. As an analogy, Nielson ratings used in the television market enable television networks to measure the popularity of individual shows and, in turn, the success of the particular network. The Nielson system collects

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

demographic information and viewing habits of television viewers by requesting viewers to voluntarily participate. Such requests are typically made through the U.S. postal service.

The Internet market has made various attempts to address the problem of measuring the effectiveness of a website. A typical unsophisticated approach uses the "hit" metric to measure the number of times a website is viewed by a user. A more sophisticated approach uses typical Internet marketing systems which track the behavior of users without their consent to achieve an unrelated objective of focusing advertisements to a user based on tracking the user's patterns of usage of the Internet. These marketing systems typically involve extracting demographic and behavior information from the user without the user's knowledge. The lack of agreement by the user raises privacy issues. Additionally, these marketing systems use the extracted information to transmit focused advertisements to the user. Besides the privacy issues raised, the lack of agreement by the user may affect the user's bandwidth because the user has no control over when data is uploaded to these marketing systems and when advertisements are downloaded to the user.

The present invention relates generally to methods and systems for using a computer to gather information regarding an end user's visits to web pages and a duration and date of each visit, and then pairing this data with the user's demographic data. Such methods and systems may suitably include the steps of monitoring the web pages that the end user visits; recording the duration and date of each visit monitored; saving information recorded in the end user's computer; storing the end user's demographic data in the data processing computer; acquiring the end users' consent to upload saved information; and uploading stored information upon selective operation by the end user from the end user's computer to the data processing computer.

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

The Art Rejections

All of the art rejections hinge on the application of either Haitsuka, Robinson, and Shear in combination, or such references further in combination with one or more of the additional references Kunzinger, Davis, and Thomas. As addressed in greater detail below, these references do not support the Official Action's reading of them and the rejections based thereon should be reconsidered and withdrawn. Further, the Applicant does not acquiesce in the analysis of these references made by the Official Action and respectfully traverses the Official Action's analysis.

Claims 1 and 3 were rejected under 35 U.S.C. §103(a) based on Haitsuka in view of Robinson and further in view of Shear. Haitsuka addresses methods and apparatus for monitoring on-line activities of an on-line user in order to display advertisements targeted to the user's on-line activities. Haitsuka, col. 3, lines 1-19. The text at col. 4, lines 42-43 of Haitsuka discloses a monitoring server 130 disposed in a network to perform user activity monitoring along with a client monitoring application 110 running on a user's machine. Each time the user performs on-line activity, the client monitoring application communicates with the monitoring server. Haitsuka, col. 5, lines 44-58. This simultaneous communication between the client monitoring application 110 and the monitoring server 130 during the time the user is on-line results in a degradation of available bandwidth to the user's on-line activity. While the user is on-line, the monitoring server determines which targeted data needs to be sent to the client monitoring application and then transmits this targeted data to the client monitoring application without any authorization by the user. See, Haitsuka, col. 6, lines 62-66.

In contrast to Haitsuka, the present invention addresses gathering information at the user's computer for subsequent reporting to a data processing computer at a time selected by the user. In

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

one aspect, the present invention addresses an advantageous approach to minimizing the degradation of user bandwidth presented by Haitzuka's approach. As taught by the present invention, the user is prompted at the expiration of a pre-defined time interval to voluntarily upload the recorded information. Such user control allows the user to postpone any user bandwidth impact resulting from uploading the stored information. Claim 1 reads as follows:

A method for using a computer to gather information of an end user's visits to web pages and a duration of each visit, the method comprising the steps of:

- (a) monitoring the web pages the end user visits;
- (b) recording the duration and date of each visit monitored in said step (a);
- (c) saving information recorded in said step (b) in the end user's computer;
- (d) acquiring the end users' consent to upload saved information; and
- (e) uploading saved information upon selective operation by the end user from the end user's computer to a data processing computer, the information saved to the end user's computer in said step (c). (emphasis added)

The Official Action cites col. 5, line 23 – col. 6, line 3, and col. 6, line 34-45 of Haitzuka as standing for the uploading step. However, Haitzuka states at col. 5, lines 44-50 that “[e]ach time an individual uses the local device 100 to connect to the data access network 120, the client monitoring application 110 and the monitoring server establish a session. In this session, the client monitoring application 110 transmits certain information regarding the user of the local device 100 and his use of the local device 100 while connected to the data access network 120.” Additionally, Haitzuka at col. 6, lines 42-45 states “[e]ach time the local device 100 connects to the monitoring server 130, the client monitoring application 110 preferably sends data indicating the local device's current geographical location to the monitoring server 130.” Accordingly, Haitzuka does not teach and does not suggest uploading information upon a “selective operation by the end user” as claimed in claim 1. Also, Haitzuka does not teach and does not suggest acquiring the end users' consent to upload saved information as claimed in claim 1. See also

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

claim 8 which requires "requesting the end user to upload the saved information upon expiration of a user defined time interval, the saved information further including URLs the user has previously visited and the duration of time the user has spent visiting these URLs." See claim 10 which requires "said processor operating to periodically request the user at the expiration of a predefined time interval to consent to uploading the monitored information to a data processing computer through the Internet". (emphasis added) See also claims 16 and 20 which require that "said monitored information is received after acquiring consent to upload said monitored information from an end user".

Further, referring to col. 6, lines 18-27 and Fig. 3 of Haitsuka, the information analyzed by Haitsuka's system is used to then send data, in the form of advertisements, to the user according to scheduling constraints. Unlike Haitsuka, the present invention advantageously transmits data in one direction from the user to the data processing computer to assess the effectiveness of web sites without subjecting the user to advertisements. Haitsuka does not teach and does not suggest uploading information "without receiving any information from the data processing computer to be displayed to the end user" as claimed in claim 8. See also claim 17 which requires the data system to only "receive monitored information without transmitting any information which would be displayed to an end user."

Robinson fails to cure the deficiencies of Haitsuka as a reference. Robinson addresses a system and apparatus for determining which advertisement to display to a particular on-line user. Robinson, col. 2, lines 9-17. To this end, Robinson's approach involves classifying users having similar interests into a "community" on the theory that people with similar interests would likely be interested in the same advertisements. Robinson, col. 2, lines 20-27. At col. 2, lines 48-57,

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

Robinson's disclosure suggests means of tracking user's activities such as the use of "cookies." Notwithstanding Internet browser configuration options which affect the Internet browser's general behavior with respect to cookies, the cookie model of programming involves a Web server fetching the information stored on the user's machine without providing the user the option to not release the cookie information. See the Understand Cookies section and the Usefulness of Cookies section of *Using Cookies* available at http://studio.tellme.com/vxml2/ovw/cookies.html#cookies_101. The remainder of the cited portion of Robinson does not teach and does not suggest "uploading saved information upon selective operation by the end user from the end user's computer to a data processing computer" as claimed in claim 1. Similarly, see claim 10 which requires that said processor "periodically requests the user at the expiration of a predefined time interval to consent to uploading the monitored information to a data processing computer through the Internet." See also claims 16 and 20 where claim 16 requires that "said monitored information is received after acquiring consent to upload said monitored information from an end user" and claim 20 requires that "said monitored information being received after acquiring consent to upload said monitored information from an end user."

The Official Action admits that Haitsuka and Robinson do not teach acquiring the end users' consent to upload saved information. The Official Action suggests paragraphs [0009]-[0047] and [0074]-[0077] of Shear as teaching a "method for obtaining user consent prior to transmitting use metering data." Applicant respectfully disagrees.

Shear fails to cure the deficiencies of Haitsuka and Robinson as references. Shear addresses the problem of securing computer environments by providing a trusted verifying

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

authority for testing load modules or other executables to verify that the load modules or other executables are accurate and complete before digitally signing them. Shear, Abstract and paras. [00033], [0036], and [0037]. To this end of securing software content such as load modules and other executables, Shear's approach includes a trusted verifying authority whose responsibilities may range from simply authorizing the origination of the load modules via a digital signature to analyzing, validating, verifying, inspecting, and testing the load modules before digitally signing them. Shear, para. [0037]. Referring to Fig. 1 and paragraph [0076] of Shear, the trusted verifying authority 100 is independent of the authorized provider 52 and consumers 56a-56c of the load modules. Further, a receiving execution environment protects itself by deciding based on digital signatures, which load modules or other executables it is willing to execute. Shear, para. [0041]. Shear's approach addresses an entirely different problem of securing software content rather than the problems of alleviating user bandwidth degradation or ensuring user privacy when gathering information of end user's visits to web pages. Further, Shear's approach provides no end user control for uploading data.

Unlike Shear, the present invention provides the end user with control over whether to upload saved information by acquiring the end user's consent before uploading. See independent claims 1, 10, 16, and 20. Shear addresses an all together different problem in an all together different manner than the present invention. Thus, there is no motivation to combine Shear with Haitsuka and Robinson.

Haitsuka, Robinson, and Shear, taken separately or in combination, do not teach and do not suggest "acquiring the end users' consent to upload saved information; and uploading saved information upon selective operation by the end user from the end user's computer to a data

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

processing computer" as claimed. Shear merely addresses securing software content regardless of obtaining an end users' consent.

Haitsuka, Robinson, and Shear cannot simply be combined with the benefit of hindsight knowledge of the invention to obtain the claimed invention. By way of example, if the teachings of Shear and Robinson were combined into Haitsuka as the Official Action suggests, the problem of decreasing user bandwidth caused by involuntary transmission of monitored information and unsolicited advertisements would still exist. Further, the problem of user privacy would still exist.

Dependent claims 4, 6, and 7 were rejected under 35 U.S.C. §103(a) based on Haitsuka, Robinson, Shear, and Kunzinger. Kunzinger describes a system which concurrently displays a set of web pages in a distributed database with a minimum of user interactions to improve the use of bookmarks in web browsers. Kunzinger, Abstract. To this end, Kunzinger's web server compresses and decompresses related web pages for concurrent display. Kunzinger, col. 9, lines 22-24.

Unlike Kunzinger, the present invention compresses and encrypts information monitored and saved at an end user's system. Claim 4 which depends on claim 1 recites "wherein the information saved in step (c) is compressed and encrypted." Step (c) in claim 1 recites "saving information recorded in said step (b) in the end user's computer." Kunzinger does not suggest and does not teach compression and encryption in the manner claimed in claim 4.

Moreover, unlike the present invention, Haitsuka's approach does not teach and does not suggest ensuring privacy by uploading saved information containing a user identification code that relates to the end user's demographic information stored at a data processing system. (emphasis added). This feature in the present invention provides end user privacy because the end user code

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

itself contains no information related to the end user which could be tapped by attaching a network analyzer monitoring network transmissions. Claim 6 recites "wherein the information saved in said step (c) is stored under an end user's user identification code." Claim 11 requires that the "monitored information is paired with end user's user identification code." Claim 15 requires "a second database for storing user identification information including a user identification code, said user identification code is used as a key to relate corresponding monitored information in the first user database with the user identification information." Claim 18 requires "the demographic information and the monitored information include an end user identification code for matching monitored information with demographic information." Claim 21 requires "comparing an end user identification code stored with the end user information with an end user identification code carried in the uploaded monitored information."

Dependent claims 8, 9, and 11-13 were rejected under 35 U.S.C. §103(a) based on *Haitsuka, Robinson, Shear, Kunzinger, and Davis*. The Official Action summarily rejected claims 10, 15-18, and 20-22 on the same grounds as claims 1, 3, 4, 6-9 and 11-14. *Davis* describes a method for monitoring a client interaction with a resource downloaded from a server in a computer network. *Davis, Abstract*. To this end, *Davis's* approach includes embedding a tracking program with the downloaded resource. The tracking program starts a timer while the user uses the downloaded resource. When the downloaded resource is a web page, once the user leaves the web page the tracking program sends the monitored time to another computer on the Internet for storage and analysis. See *Davis*, col. 9, lines 3-15. Because the tracking software is embedded in the downloaded resource, a user of *Davis's* system is unaware of the information gathered and the event of the timer being expired and is not provided timing control of the uploading information.

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

In stark contrast to Davis, the present invention acquires the user's consent for uploading monitored information. For example, the user may log on to the system before each web session by identifying himself or herself as shown in Fig. 2 by providing the user's identification code or user name. See page 11, lines 7-11. Further, referring to page 7, lines 6-9, the user by other means than the network registers personal demographic information for entry into the global user demographic database to ensure privacy and consent, for example. The present invention's data processing center 22 "never prompts an end user to upload any information and never receives any data unless the user voluntarily uploads the data." Specification, page 11, lines 31-33. See independent claim 10 which requires "said processor operating to periodically request the user at the expiration of a predefined time interval to consent to uploading the monitored information to a data processing computer through the Internet", independent claim 16 which requires "said monitored information being received after acquiring consent to upload said monitored information from an end user", and independent claim 20 which requires the step of "receiving uploaded monitored information from an end user's computer wherein said monitored information including the URLs visited by end users and the duration of time spent visiting these URLs, said monitored information being received after acquiring consent to upload said monitored information from an end user."

Davis, separately or in combination with the other references, does not teach and does not suggest acquiring the consent to upload monitored information from an end user as claimed. Davis simply embeds a tracking program with the downloaded resource to be tracked. For Davis to accomplish the objectives of the present invention, Davis's tracking software must be installed on all resources intended to be tracked. The present invention takes an entirely different approach

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

by tracking voluntary users' habits to accumulate ratings for visited web sites, a problem which is not addressed in Davis. These accumulated ratings may be subsequently sold to the URLs visited by the voluntary users.

Dependent claims 14 and 19 were rejected under 35 U.S.C. §103(a) based on Haituka, Robinson, Kunzinger, Shear, Davis, and Thomas. The Official Action summarily rejected claims 10, 15-18, and 20-22 on the same grounds as claims 1, 3, 4, 6-9 and 11-14. Thomas describes a system for customizing web pages based on demographic information stored on a client's computer. The Official Action apparently relies upon Thomas for its disclosure related to encrypting and compressing demographic information.

Unlike Thomas, the present invention not only does not compress demographic information, it does not upload demographic information over the network. Demographic data is supplied off-line to the data processing center for input to the global user demographic database, for example, during a registration process over the telephone or by conventional mail. Specification, page 7, lines 6-9. The Official Action misreads the present invention. The present invention uploads a user identification code which is mapped to demographic information at a global user demographic database. There are no presently pending claims which claim compressing demographic information. Thus, Thomas is irrelevant to the present claims.

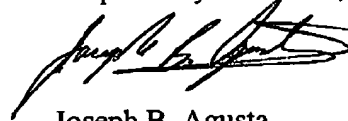
The relied upon references fail to recognize and address the same problems in the manner advantageously addressed by the present claims. The claims as presently amended are not taught, are not inherent, and are not obvious in light of the art relied upon.

Appl. No. 09/497,006
Amdt. dated March 4, 2004
Reply to Office Action of December 4, 2003

Conclusion

All of the presently pending claims define over the applied art. The present rejections should be withdrawn and the claims promptly allowed.

Respectfully submitted,



Joseph B. Agusta
Reg. No. 52,547
Priest & Goldstein, PLLC
5015 Southpark Drive, Suite 230
Durham, N.C. 27713-7736
(919) 806-1600